STANDARD

RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED FOR THE PURPOSE OF MANAGING HEALTH VIGILANCE SYSTEMS

In the event of any inconsistencies between the French adopted version and this English courtesy translation, please note that the French version shall prevail.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. To whom is this standard addressed?

This standard exclusively applies to the processing of personal data:

- carried out in order to manage health vigilance systems;
- and implemented by manufacturers, companies, operators ("exploitants") and organisations responsible for placing a medicine, a device or a product on the market and referred to hereinafter as the controller.

Pursuant to Article 65 1° of the amended Act of 6 January 1978 (hereinafter the French Data Protection Act), the processing of personal data implemented by health professionals and health care systems or services (for example: health care establishments, health care homes, health care centres, sanitary care agencies, etc.) are not concerned by this standard.

2. Scope of the standard

This standard specifies the legal framework resulting from the General Data Protection Regulation (GDPR) and the national provisions which are applicable to the processing of personal data carried out in the context of health vigilance systems. It covers the vigilance systems mentioned in the ministerial Order of 27 February 2017 establishing the list of categories of adverse sanitary events for which reporting or notification can be may be made through the portal for reporting adverse sanitary events.

Controllers which send a notification of compliance to the CNIL for the processing of personal data meeting the requirements set by this standard, by using the form for notification of compliance to be completed on the CNIL's website, are authorised to implement such processing operations.

On the other hand, any processing of personal data exceeding the framework or the requirements set out by this standard must apply for an authorisation in accordance with Article 66-III of the French Data Protection Act.

Controllers must implement all appropriate (technical and organisational) measures in order to ensure the data protection by design and by default. Moreover, they must demonstrate compliance throughout the duration of the processing operations. The processing implemented within the framework of this standard must also be recorded in the record of processing activities provided for in Article 30 of the GDPR (see the template of records of processing activities on the CNIL's website cnil.fr).

The principles set by the CNIL in this standard constitute an aid for carrying out the data protection impact assessment that controllers must perform. Controllers may thus define the measures allowing them to ensure the proportionality and the necessity of their processing (points 3 to 7 of the standard), to guarantee the data subjects' rights (points 8 and 9 of the standard) and risks management (points 10 to 12 of the standard).

3. Aim(s) of the processing (purposes)

The purpose of a processing that is implemented in order to manage health vigilance systems is to allow for the prevention, monitoring, assessment and management of adverse sanitary events, as set up by the controller.

The processing is intended to allow:

- the collection, recording, analysis, monitoring, documentation, transmission and retention of the data relating to all adverse sanitary events;
- the management of contacts, by the controller with the individual who reported the adverse sanitary event (a member of an approved association, a healthcare professional, a member of a health authority, a patient, etc.) or the healthcare professional who may be questioned in order to obtain clarifications concerning the reported adverse sanitary event in compliance with medical secrecy (the professional taking care of the person who is suffering the adverse sanitary event, etc.).

The information collected for this purpose may not be further processed for any other purpose than those provided by this standard.

4. Legal basis for the processing

Compliance with legal obligations imposed on the controller by, notably, the French Public Health Code concerning health vigilance systems are considered as the legal basis for the processing of personal data.

The collection of health data in connection with health vigilance systems is necessary for reasons of public interest. In particular, it is intended to ensure high standards of quality and safety of health care and of medicine, medical devices or products in accordance with Article 9 of the GDPR and Article 66 of the French Data Protection

5. Personal data concerned

Only data that are relevant with regard to the processing's aim, namely the management of health vigilance systems, may be collected and processed. In this regard, the controller may collect and process the following data, depending on the processing's aim and the situations:

a) Data concerning the exposed person that are strictly necessary in order to assess the adverse sanitary event:
   - data which allow indirect identification of the person exposed to the adverse sanitary event (descriptive information such as age, year or date of birth, sex, weight, height) or the identification number of the person (alpha-numeric code, alphabetical identification code, as provided for by the existing forms) and which allow the person's privacy to be guaranteed, and excluding any national identification number for natural persons and the national health identifier;
   - data relating to the identification of the product concerned by the report of the adverse sanitary event: type of medicine, type of device or product used, serial number, etc.;
   - health data, notably: treatments administered, examination results, nature of the adverse event or events, personal or family history, illnesses or associated events, risk factors, information concerning the method of prescription and use of medicines, and the therapeutic conduct of the prescriber or the healthcare professionals participating in the treatment of the illness or the adverse sanitary event.

     In addition to those data, the controller may also collect and process other data, provided that they are strictly necessary in order to assess the adverse sanitary event (professional life, consumption of tobacco, alcohol, drugs, life habits and behaviour). Data revealing ethnic origin may be collected by the controller when a document presenting the characteristics of the medicine, device or product validated by a competent authority (e.g. summary of characteristics for medicines, summary of characteristics for medical devices, etc.) states, on the basis of scientific knowledge, that the data subjects' ethnic origin may have an impact on its efficacy or safety.

b) The contact details of the person who reported the adverse sanitary event or any healthcare professional who may provide any clarifications (first name, surname, postal address, electronic address, telephone number and, if appropriate, the speciality of the healthcare professional). Depending on the situation, the person who made the report may be: a member of a health authority, a healthcare professional, the person exposed to the adverse sanitary event or his/her relatives, the holder(s) of parental responsibility, the right-holder in the case of death, or an approved association of patients, etc. When the report of the adverse sanitary event is made directly by the exposed person, it has the effect of lifting the secrecy of his/her identity and should be limited to what the controller needs to know in order to satisfy its vigilance duties and for a duration that is strictly limited to what is necessary in order to satisfy these obligations.

6. Recipients of the data

Only the authorised employees of the controller, acting under the responsibility of the controller, may access the personal data, within the limit of their respective roles and to the extent which concerns them, notably:

- the person in charge of the vigilance system, as well as his/her colleagues and officers participating in the process of managing health vigilance;

- the personnel of the audit service, for a specific and justified reason, in order to verify compliance with the regulatory requirements;
- authorised personnel in charge of managing claims, in consideration of the cases that they have to handle.

The following may also receive the data necessary to perform their tasks, exclusively in connection with their vigilance activities:

- processors acting on behalf of and under the responsibility of the controller, within the limits of their functions and under the conditions defined by the processing agreement. If a processor is used, the agreement between the controller and the processor must state the processor's obligations in terms of data protection (Article 28 of the GDPR). The guide for processors published by the CNIL specifies their obligations and the clauses to be included in the agreements;
- other companies of the group to which the organisation belongs and which participate in the exploitation or marketing of the medecine, the device or the product in question;
- third parties whose medecine, device or product may be involved, with the exception of data that directly identify the person exposed to the adverse sanitary event and who reported the event;
- the healthcare professionals participating in monitoring the patient and the healthcare or other professionals who may provide additional information;
- notified bodies in charge of assessing a medecine, device or product, except for the data that directly identify the exposed person to the adverse sanitary event and who reported the event;
- the national pubic authorities (for example: regional health agencies ("*agences régionales de santé*"), health agencies, etc.) or foreign public authorities in charge of product surveillance as part of carrying out their missions as defined in the texts, the foreign national health authorities or agencies and the international health authorities or agencies (e.g. the European Medicines Agency), except for data that directly identify the exposed person who reported the event.

7. Retention period

The data collected and processed for the purpose of managing health vigilance may not be retained indefinitely. A precise retention period must be set in advance and in consideration of the purpose of the processing.

With regard to the processing's purpose, the data are retained in an active data base for the duration of the current use of the data. They are then retained in an intermediary archive for the legal or regulatory duration applicable to each case of health vigilance. In the absence of a legal or regulatory duration, data should not be retained beyond a period of seventy years from the removal of the medicine, device or product from the market.

Upon expiry of these retention periods, the data must be erased or archived in an anonymised form.
The retention and archiving of the data must be carried out under security conditions that are in accordance with Article 32 of the GDPR.

8. Information of data subjects

Processing of personal data must be implemented with full transparency with regard to the data subjects (the persons exposed to the adverse sanitary event, the person who reported the adverse sanitary event and the healthcare professional monitoring the exposed person). The controller must take appropriate measures in order to provide concise, transparent, comprehensible and easily accessible information in clear and simple terms to the data subject.

As from the collection stage, the data subjects must be informed individually of the conditions of the processing of their data, in accordance with the requirements provided for in Article 13 and, if appropriate, Article 14 of the GDPR and Articles 69 and 70 of the French Data Protection Act.

In case of notification of an adverse sanitary event by the exposed person, specific information must be provided to him/her in advance in order to inform him/her that his/her identity will not be kept confidential.

The means of providing this information are free (either orally or in writing).

If the data subject requests, he/she may obtain the provision of information by way of written material.

In case of an adverse sanitary event's notification by a person other than the exposed person, the information is provided to him/her by the reporting person on the basis of the written information provided to the reporting person by the controller.

The controller must demonstrate at all times that the information was delivered to the data subjects, with the controller being responsible for obtaining proof of this delivery from the reporting person.

In addition, the data subjects must be informed of the procedure for exercising their rights.

9. Data subjects' rights

The data subjects (the persons exposed to the adverse sanitary event, the person who reported the adverse sanitary event and the healthcare professional monitoring the exposed person) have the following rights that they may exercise under the conditions provided for by the GDPR:

- the right of access;
- the right to rectification;
- the right to restriction of processing (e.g. when the data subject contests the accuracy of his/her data, he/she may request the controller to temporarily freeze his/her data while the controller undertakes the necessary verifications).

As the processing is based on compliance with a legal obligation, the data subjects concerned by the collection of data do not have a right of objection, a right to erase the data or the right to data portability. The data subjects must be informed of this in advance.

10. Security

In general, the controller must take all appropriate measures with regard to the risks presented by the processing in order to preserve the security of the personal data and, notably at the time of collection, during their transmission and their retention, to prevent them from being distorted, damaged or accessed by unauthorised third parties.

In particular, in the specific context of this standard, the controller must either adopt the following measures or demonstrate equivalent measures or demonstrate that it does not have a need to or cannot use such measures:

Categories	Measures
Training users	Informing and raising awareness of the persons handling the data
	Preparing an IT policy and giving it binding force
Authenticating users	Defining a unique identifier (login) for each user
	Requiring the user to change his/her password after resetting
	Using a strong authentication method relying on a verified directory
	Limiting the number of attempts to access an account
	Adopting a user password policy in accordance with the recommendations of the CNIL
Managing authorisations	Defining the authorisation profiles
	Carrying out an annual review of authorisations
	Deleting obsolete access authorisations

Logging access and managing incidents	Providing for a logging system
	Providing for procedures for reporting personal data breaches
	Informing users that a logging system has been put in place
	Protecting the logging equipment and the logged information
Securing work stations	Providing for an automatic procedure to lock the session
	Collecting the consent of the user before any remote intervention on his/her equipment
	Using regularly updated anti-virus software
	Installing a software firewall
Securing the mobile equipment	Providing for means of encryption for mobile equipment
	Requiring a secret answer for unlocking smart phones
	Making regular backups or synchronisations of the data
Protecting the internal information network	Limiting the network flows to what is strictly necessary
	Implementing WPA2 or WPA2-PSK protocol for Wi-Fi networks
	Securing remote access to mobile computing devices by VPN
Securing the servers	Limiting access to the administrative tools and interfaces solely to authorised persons
	Ensuring the availability of the data
	Installing critical updates without delay
Securing the websites	Using the TLS protocol and verifying its implementation
	Implement a banner for consent to trackers (cookies) that are not necessary for the service
	Verifying that no password or identifier passes through the URLs
	Checking that the entries by users match what is expected
Protecting and providing for business continuity	Making frequent backups of the data, whether in paper or electronic form
	Planning and regularly testing business continuity
	Storing the backup media in a safe location
	Providing for secure means for transport of backups
Archiving in a secure manner	Implementing specific conditions for access to the archived data Destroying obsolete archives in a secure manner
Managing the maintenance and destruction of data	Logging the maintenance interventions in a log book
	Deleting the data from any equipment before it is discarded
	Managing interventions by third parties under the supervision of a person from the organisation
Managing the use of processors	Providing for a specific clause in the processors' agreements
	Ensuring the effectiveness of the guarantees provided (security audits, inspections, etc.)

	Providing for conditions for the return and destruction of the data
Securing the exchanges with other organisations	Sending the data in encrypted form (either direct encryption of the data or by using an encrypted channel)
	Transmitting the secret by a separate message and via a different channel
	Ensuring that the recipient is the right one
Protecting the premises	Restricting access to the premises by means of locked doors, either to paper files or computer equipment, notably the servers
	Installing intruder alarms and verifying them periodically
Managing the software developments	Proposing privacy friendly settings to the end users
	Testing on fictional or anonymised data
	Avoiding free tex areas or managing them strictly
Using cryptographic functions	Using recognised algorithms, software and libraries
	Retaining the secrets and the cryptographic keys in a secure manner

In order to do so, the controller may refer to the Guide for the Security of Personal Data published by the CNIL.

Any personal data breach must be reported to the CNIL under the conditions provided for by Article 33 of the GDPR.

If the controller uses an external service provider for the storage and retention of the personal health data, this service provider must be an approved or certified health data hosting provider. By way of exception, when the controller is not established in France, the controller must demonstrate that the service provider that it uses offers equivalent security guarantees.

The service agreement should be compliant with the conditions provided for in Article 28 of the GDPR.

11. Transfer of data outside of the European Union

Data which indirectly identify the exposed persons and the data which directly identify the reporting persons may be transferred outside of the European Union if the following conditions are met:

- Compliance with the provisions of Article 6 concerning the recipients of the data;
- the transfer of data is strictly necessary for the implementation of the vigilance system.

The transfer may be made within the framework of the notification of compliance with this standard when one of the following conditions is met:

- the transfer is made to a country or an international organisation recognised by the European Commission as ensuring an adequate level of protection, in accordance with Article 45 of the GDPR (adequacy decision);
- the transfer is made using the appropriate safeguards as listed in Article 46, paragraph 2, of the GDPR (i.e. standard contractual clauses approved by the European Commission, binding corporate rules, code of conduct, certification mechanism);
- in the absence of a decision of adequacy or appropriate safeguards, the transfer may be based on one of the exceptions provided for in Article 49 of the GDPR when such a transfer is not repetitive, massive or structured.

The controller must inform the data subjects in advance of the transfer of their personal data to countries outside of the European Union, the existence or the absence of an adequacy decision or an appropriate safeguard and the means for obtaining a copy of this in accordance with Article 13, paragraph 1, point f, of the GDPR.

12. Privacy Impact Assessment (PIA)

Pursuant to article 35 of the GDPR, the controller must carry out a privacy impact assessment.

In order to carry out this impact assessment, the controller may refer to:

- the principles contained in this standard;
- the methodological tools made available by the CNIL on its website.

If necessary, the Data Protection Officer (DPO) must be consulted.
In accordance with article 36 of the GDPR, the controller must consult the CNIL before implementing the processing if, following the impact assessment, it is not able to identify measures that are sufficient in order to reduce the risks to an acceptable level (the residual risk remains too high).